

WHAT IS YOUR DATA-FLOW NARRATIVE?

A data-flow diagram gives account data a route. A data-flow narrative gives every route a transaction, condition, data state, owner, and consequence. If the arrow cannot be spoken as a complete testable sentence, it may be decoration.

PRACTITIONER POSITION

PCI DSS v4.0.1 Requirement 1.2.4 requires an accurate data-flow diagram or other technical or topological solution that shows all account-data flows across systems and networks and is updated as the environment changes. My practitioner position is that the diagram is necessary topology, but it rarely carries the complete operating meaning an entity and assessor need. A governed data-flow narrative complements the diagram by describing who or what initiates each flow, the business event, exact account-data state, source and destination, interface and protocol, trust boundary, protection and transformation, storage or buffering, authorization boundary, retention or deletion, provider responsibility, failure and fallback paths, evidence, and scope consequence. It does not replace the diagram. It makes the diagram interrogable. Every narrative step should map to stable node and edge identifiers, and every material diagram edge should resolve to at least one current narrative statement. The diagram answers where account data can go. The narrative explains what happens there, under which conditions, and why the resulting PCI claim is supportable.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

The payment diagram is clean: Browser -> Web Tier -> Processor. The assessor asks whether the browser posts PAN directly to the processor, whether the web tier can influence the payment page, what happens when tokenization times out, where retries queue, how refunds are initiated, whether logs receive payload fragments, who administers the processor integration, and when SAD leaves memory. The three arrows cannot answer. The application owner begins drawing new boxes from memory: a tag manager, support console, webhook receiver, dead-letter queue, observability service, fraud provider, mobile client, batch export, and emergency fallback. The diagram was not necessarily false. It was semantically incomplete, and the missing meaning carried scope.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- Arrows have no stable identifiers, owners, business events, data classifications, or evidence references.
- One happy-path purchase diagram is expected to represent refunds, reversals, retries, failures, support access, recurring payments, mobile use, and batch operations.
- The same label-payment data, encrypted data, or token-is used for PAN, SAD, tokens, truncated PAN, hashes, and provider identifiers.

- The authorization-completion point is unknown, so nobody can explain when retention of SAD becomes prohibited.
- Logs, traces, queues, caches, crash dumps, screenshots, exports, and support artifacts are absent because nobody intended them as payment stores.
- TPSP arrows end at a company name instead of an exact service, interface, responsibility boundary, and customer-controlled configuration.
- The diagram is updated annually while interfaces, payment scripts, identities, provider services, and failure behavior change continuously.
- People can explain the flow in a meeting, but the explanation is not versioned, cross-referenced, testable, or available to the next operator or assessor.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Start with stable nouns and verbs. Give systems, services, stores, actors, trust boundaries, and external parties durable node identifiers. Give each permitted transfer or influence path an edge identifier and a precise verb such as sends, redirects, renders, tokenizes, stores, retrieves, logs, administers, or can change. Browser to processor is a line. BROWSER-01 submits PAN directly to TPSP-PAY-01 through hosted field HF-02 over TLS after SCRIPT-04 renders the page is a statement that can be challenged.

Describe data state at each step. Account data does not remain one undifferentiated substance. Record whether a step involves PAN, SAD, token, truncated PAN, keyed hash, transaction identifier, or non-account metadata; whether it is clear, encrypted, masked, transient, retained, or derived; and which event changes that state. Encryption can protect data without removing it from scope. Tokenization can alter downstream applicability without erasing the systems that can influence capture or detokenization.

Narrate the ordinary path and every material alternate path. Include decline, timeout, retry, offline or fallback behavior, reversal, refund, recurring transaction, support and troubleshooting, batch export, dispute, fraud review, application error, queue failure, and provider outage where they exist. Alternate paths are often where data lands in temporary stores, error messages, observability, or manual procedures that the happy-path picture never reveals.

Make time visible. State when capture begins, when authorization completes, how long buffers and queues persist, which retention clock applies, when logs rotate, when deletion occurs, and how the entity proves those events. A static arrow can conceal that SAD is legitimate during transaction processing and prohibited after authorization. A narrative can bind that transition to a measurable event and evidence source.

Bind TPSP participation to the exact service and shared-responsibility seam. Name which party hosts the interface, controls DNS and scripts, receives data, manages encryption keys, administers identities, retains records, monitors failures, and supplies evidence. Vendor handles payment is not a narrative. It is an untested conclusion with the verbs removed.

Reconcile the narrative with the scope graph, component inventory, network and architecture diagrams, software inventory, data stores, public edge, identity plane, provider register, and testing populations. A narrative edge that references an unknown component is an inventory discrepancy. A diagram edge without

a narrative is unexplained behavior. A scan target, test subject, or provider connection that cannot resolve to either is a coverage question.

Version the narrative with the architecture it explains. Record effective dates, approver, evidence, change triggers, and supersession. Reopen affected statements when payment code, interfaces, scripts, DNS, routes, identities, provider services, failure modes, storage, logging, or administrative control changes. Do not overwrite yesterday's truth; an assessment period may need to explain more than one effective flow state.

Use narrative review as an operational exercise. Ask an application owner, network owner, payment owner, provider owner, and assessor to independently walk one transaction from capture through deletion and one failure path. Differences are not editorial annoyances. They are evidence that the entity does not yet share one complete scope story.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 Can every diagram node and edge be referenced by a stable identifier in the narrative?
- 02 For each flow, who or what initiates it, which business event triggers it, and which party owns it?
- 03 Which exact account-data elements and states exist before, during, and after every transformation?
- 04 Where are the authorization boundary, transient stores, queues, logs, retries, exports, and deletion events?
- 05 Which failure, fallback, support, refund, reversal, recurring, and dispute paths differ from the ordinary transaction?
- 06 Which TPSP service participates, which responsibilities remain with the entity, and which evidence supports the seam?
- 07 Which inventory, scope, scan, test, identity, and evidence records cross-reference each step?
- 08 What change reopens a narrative statement, and can the entity reconstruct the flow that was effective during the assessment period?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Collect current data-flow, network, application, sequence, and provider diagrams; payment journeys; interface specifications; inventories; logs; queue and storage configurations; failure procedures; and the explanations operators currently carry in their heads.

02 / MAP

Create a Data-Flow Narrative Ledger. Bind each statement to node IDs, edge ID, actor, trigger, data element and state, source, destination, interface, trust boundary, protection, transformation, persistence, authorization event, owner, TPSP responsibility, evidence, and scope consequence.

03 / EXPLAIN

Write the ordinary flow and material alternate flows as complete sentences. Separate observed behavior, documented design, PCI SSC source language, assessor judgment, and practitioner interpretation.

04 / REDUCE

Remove duplicate diagrams, vague data labels, unexplained arrows, oral-only exceptions, invisible failure stores, and company-name TPSP endpoints. Generate different views from one governed relationship model where practical.

05 / PROVE

Select one diagram edge and trace it through live configuration, an observed transaction or safe test, logs, provider evidence, retention behavior, inventory, scope conclusion, and required testing. Then inject a failure and show which new path appears.

THE FIELD LAW

THE LINE WORTH REMEMBERING

A DIAGRAM SHOWS THE ROUTE. A NARRATIVE EXPLAINS THE TRANSACTION AND ITS CONSEQUENCES.

Download the Data-Flow Narrative and Diagram Reconciliation. Give every material arrow a complete sentence, data state, owner, evidence reference, and scope consequence. Then find every sentence that has no arrow and every arrow that has no sentence.

TECHNICAL GROUNDING

START WITH THE SOURCE MATERIAL

These references ground the practitioner interpretation. They do not turn the metaphor or method into official PCI DSS terminology.

- WACK-SOURCE-0001 / PCI DSS v4.0.1 / PCI Security Standards Council / [Open source](#)

- WACK-SOURCE-0005 / PCI DSS Scoping and Segmentation Guidance for Modern Network Architectures / PCI Security Standards Council / [Open source](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

Practitioner reviewed by Scott Norton on 2026-09-09 against canonical digest

50ef6c94c2d939e3914514a526bb7df6538825d7858fb2cdc5891a573cffcf22. Educational content, not a compliance determination. Independent practitioner resource; not affiliated with or endorsed by PCI SSC. Authorship and authority classification do not determine legal intellectual-property ownership.